



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.		
10/692,261	10/23/2003	Jon Cargille	MS1-1781US	1559		
22801	7590	03/04/2009	EXAMINER			
LEE & HAYES, PLLC 601 W. RIVERSIDE AVENUE SUITE 1400 SPOKANE, WA 99201				TRUVAN, LEYNNA THANH		
ART UNIT		PAPER NUMBER				
2435						
MAIL DATE		DELIVERY MODE				
03/04/2009		PAPER				

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/692,261	CARGILLE ET AL.	
	Examiner	Art Unit	
	Leynna T. Truvan	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 25 November 2008.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1, 3-7, 12-19, 21, 26-29, and 31-33 is/are pending in the application.
 - 4a) Of the above claim(s) 2,8-11,20,22-25 and 30 is/are withdrawn from consideration.
- 5) Claim(s) 1, 3-6, 15-18, 21, 26-29, and 31-33 is/are allowed.
- 6) Claim(s) 7,12-14 and 19 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

<input type="checkbox"/> Notice of References Cited (PTO-892)	<input type="checkbox"/> Interview Summary (PTO-413)
<input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
<input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____ .	6) <input type="checkbox"/> Other: _____ .

DETAILED ACTION

1. Claims 1, 3-7, 12-19, 21, 26-29, and 31-33 are pending.

Claims 2, 8-11, 20, 22-25, and 30 are cancelled by applicant.

Allowable Subject Matter

2. Claims 1, 3-6, 15-18, 21, 26-29, and 31-33 are allowed.

3. The following is a statement of reasons for the indication of allowable subject matter: the amendment of 11/25/08 made pertaining to claims 1, 3-6, 15-18, 21, 26-29, and 31-33 have overcome the previous art rejection. A further search and consideration was performed and found there are no prior art to fully disclose or support the claimed invention of 1, 3-6, 15-18, 21, 26-29, and 31-33. Therefore, these claims are in condition for allowance.

Response to Arguments

4. Applicant's arguments filed 11/25/08 have been fully considered but they are not persuasive.

Since claims 1, 3-6, 15-18, 21, 26-29, and 31-33 are in condition for allowance, their arguments will not be addressed as they have overcome art rejections.

Regarding argument on pg. 17 for claims 7, 12-14, and 19: they are not allowable because they do not recite or suggest the same limitations as

amended in the independent claims 1, 15, 21, and 29. They remain rejected over Harman, et al. (US 6,807,636) and Benantar, et al. (US 5,765,153).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 7, 12-14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harman, et al. (US 6,807,636) in view of Benantar, et al. (US 5,765,153).

As per claim 7:

Harman discloses a method of implementing a kernel-level transaction, comprising:

attaching a security descriptor to at least one of plurality of kernel objects utilized in a kernel-level transaction; and (col.14, lines 20-32 and

col.15, lines 18-35; *modules being called or loaded by the kernel are given as kernel objects)*

performing an operation for the kernel-level transaction on the at least one kernel object (col.14, lines 13-17 and col.18, lines 20-33) in accordance with the rights accorded by the security descriptor attached to the at least one kernel object, wherein the security descriptor includes identification for at least one user (col.13, lines 1-26), an operation that is able to be performed on the at least one kernel object to which the security descriptor is attached (col.18, line 59 – col.19, line 11), and a right indicating that the identified user is permitted or prohibited to perform the operation (col.20, lines 29-63), and further wherein the at least one kernel object comprises a transaction object (col.14, lines 42-50 and 58-67 and col.15, lines 36-40; *transaction module is given as security request and/or monitor associated with the application or service module*), a resource manager object (col.14, lines 30-42 and 51-52 and col.15, lines 55-67; *a resource object given as component, i.e. interface, controller, device server (col.17, lines 33-52)*) and/or an *[enlistment object]*.

Harman includes transaction object to represent a transaction which is a service module/application to plural kernel objects. The kernel-level transaction can broadly be associated to an operating system core or level. Thus, the claimed objects and transactions are obviously participates at the kernel level if they are kernel objects. However, Harman does not go into details of an enlistment object to enlist participants.

Benantar's invention improves security in object oriented system where the security system is a point of control for the security information and allows for its isolation from application programs with the goal of maintaining the integrity and the prevention of the policy from outside tampering (col.1, lines 16-30). The method includes requesting different security services managing a resource access policy, inquiring as to resource access decision, or for the subject registry (col.1, lines 37-43). Benantar discusses object oriented program include a system authorization policy object (SAP), SAO, and a system registration object (SAO) where the SAP object is used to retrieve and manipulated user capabilities that enlists the object that the user is allowed access to, along with the corresponding access types or permission (col.2, lines 54-65). the user capability enlists the objects to which the user is allowed access along with the type of access that corresponds to the method the user can execute (col.5, lines 17-25). This includes management of subject capability for environment is capability based form based for authorization. Benantar discloses the user's capability enlists the object to which the user allowed access along with the type of access that corresponds to the methods the user can execute (col5, lines 10-28). Thus, Benantar obviously suggests the claimed enlistment object to enlist participants in the transaction.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of transaction manager that includes kernel objects of Harman with enlistment object to enlist participants in the security

system of Benantar because to improve security by maintaining the integrity and the prevention of the policy from outside tampering (Benantar - col.1, lines 16-30 and col5, lines 10-28).

As per claims 8-11: cancelled

As per claim 12: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 7, wherein the operation identified by the security descriptor attached to the transaction object includes at least one of: set information regarding the transaction object, enlist the transaction object in the kernel-level transaction, render data updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the kernel-level transaction at the transaction object, and transmit data regarding the kernel-level transaction to another device.

As per claim 13: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 7, wherein the operation identified by the security descriptor attached to the resource manager object includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a kernel-level transaction at a moment of transaction failure, object, and enlist the resource manager object in a kernel-level transaction, register the resource manager

object in the kernel-level transaction, receive notification upon resolution of a kernel-level transaction at the resource manager set resource data in accordance with the kernel-level transaction resolution.

As per claim 14: Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 7, wherein the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure, obtain and reference an enlistment key, rollback the kernel-level transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 19:

Harman discloses a kernel-level transaction method, comprising:
implementing a kernel-level transaction among kernel objects; (col.14, lines 20-32 and col.15, lines 18-35; *modules being called or loaded by the kernel are given as kernel objects*)
securing the kernel-level transaction utilizing an operating system security model that applies a security descriptor to at least one of the kernel objects participating in the kernel-level transaction; (col.18, line 59 – col.19, line 11)
wherein the security descriptor includes identification for at least one user (col.13, lines 1-26), an operation to be performed on the at least one

kernel object to which the security descriptor is attached (col.14, lines 13-17 and col.18, lines 20-33), and a right indicating that the identified user is permitted or prohibited to perform the operation (col.20, lines 29-63) and each of the kernel objects comprise a transaction object (col.14, lines 42-50 and 58-67 and col.15, lines 36-40; *transaction module is given as security request and/or monitor associated with the application or service module*), a resource manager object (col.14, lines 30-42 and 51-52 and col.15, lines 55-67; *a resource object given as component, i.e. interface, controller, device server (col.17, lines 33-52)*) and/or [an enlistment object].

Harman includes transaction object to represent a transaction which is a service module/application to plural kernel objects. The kernel-level transaction can broadly be associated to an operating system core or level. Thus, the claimed objects and transactions are obviously participates at the kernel level if they are kernel objects. However, Harman does not go into details of an enlistment object to enlist participants.

Benantar's invention improves security in object oriented system where the security system is a point of control for the security information and allows for its isolation from application programs with the goal of maintaining the integrity and the prevention of the policy from outside tampering (col.1, lines 16-30). The method includes requesting different security services managing a resource access policy, inquiring as to resource access decision, or for the subject registry (col.1, lines 37-43). Benantar discusses object oriented

program include a system authorization policy object (SAP), SAO, and a system registration object (SAO) where the SAP object is used to retrieve and manipulated user capabilities that enlists the object that the user is allowed access to, along with the corresponding access types or permission (col.2, lines 54-65). the user capability enlists the objects to which the user is allowed access along with the type of access that corresponds to the method the user can execute (col.5, lines 17-25). This includes management of subject capability for environment is capability based form based for authorization. Benantar discloses the user's capability enlists the object to which the user allowed access along with the type of access that corresponds to the methods the user can execute (col5, lines 10-28). Thus, Benantar obviously suggests the claimed enlistment object to enlist participants in the transaction.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of transaction manager that includes kernel objects of Harman with enlistment object to enlist participants in the security system of Benantar because to improve security by maintaining the integrity and the prevention of the policy from outside tampering (Benantar - col.1, lines 16-30 and col5, lines 10-28).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KIM VU whose telephone number is (571)272-3859. The examiner can normally be reached on Monday through Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kimyen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435